geheim: Alternativen zum Abruf E-Rezepte mit eGK

Proof of Patient Presence (Grobkonzept)

Als Proof of Patient Presence (PoPP) bezeichnet das Grobkonzept „ein kryptografisch gesichertes Artefakt zur Prüfung der Autorisierung“.

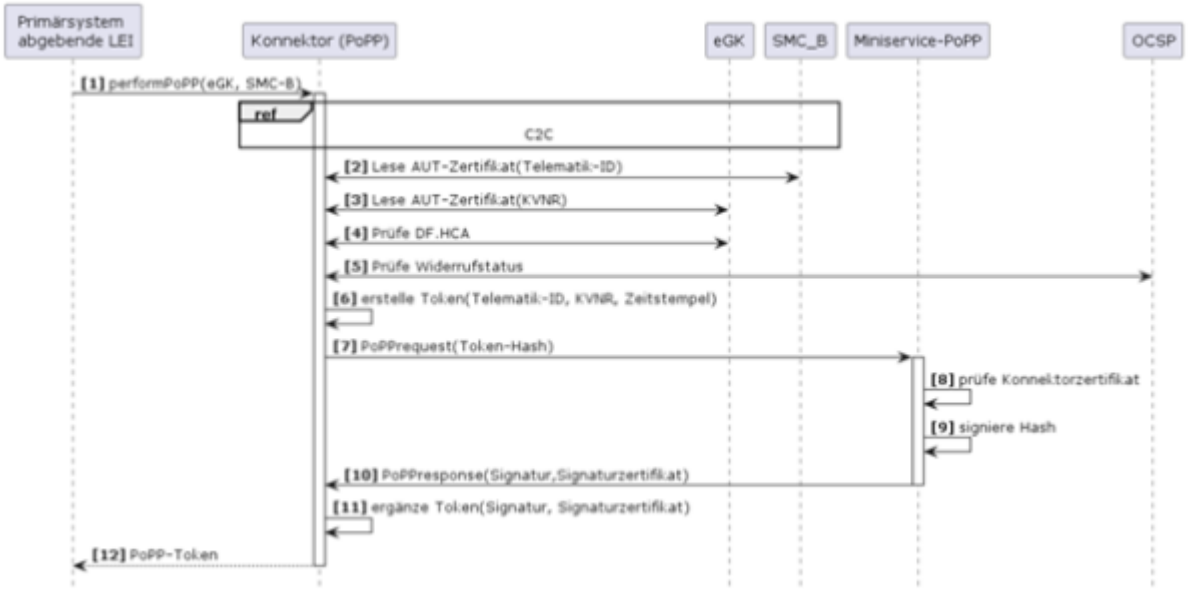
Im Rahmen der vorgeschlagenen Lösung kapselt ein sog. Miniservice-PoPP die Signaturerstellung und hält das zugehörige Zertifikat. Eine sog. Fachlogik-PoPP im (Basis-)Konnektor setzt die notwendigen Zugriffe auf SMC-B und eGK um.

Grob gesagt erstellt der Konnektor (Fachlogik-PoPP, Operation GetPoPP-Token) ein Token (bzw. dessen Hash), das folgende vom Konnektor geprüfte Testate enthält:

- KVNR der (mittels C2C zwischen SMC-B und eGK) auf Echtheit und (mittels Statusprüfung von DF.HCA und OCSP-Abfrage auf) Sperrung geprüften eGK
- Telematik-ID der SMC-B(, die zur Echtheitsprüfung der eGK verwendet wurde)
- Systemzeit der Prüfung.

Das Token sendet der Konnektor (mittels beidseitig authentifiziertem TLS verschlüsselt) an den Miniservice-PoPP zur Signatur, welcher das signierte Token an den Konnektor zurücksendet. Der Konnektor sendet das signierte Token dann abschließend an das Primärsystem zurück. Die skizzierte Lösung ist TI2.0-kompatibel, da lediglich Identifier im Token genutzt werden, die auch mit TI2.0-Technologien nutzbar sind.

Folgende Abbildung zeigt den genauen Ablauf mittels eines Sequenzdiagramms.



Das AVS nutzt dieses PoPP-Token dann zum Abruf aller offenen Rezepte für die KVNR im Token vom E-Rezept-Fachdienst. Der Fachdienst prüft dann

- die Gültigkeit der PoPP-Token-Signatur

- die Übereinstimmung der Telematik-ID im AccessToken des AVS mit der des PoPP-Token
- die zeitliche Nähe des Ausstellungszeitpunkts des PoPP-Token zum aktuellen Zeitpunkt

Ergänzend prüft der E-Rezept-Fachdienst periodisch die Gültigkeit der Signaturzertifikate des PoPP-Service.

Anwesenheitsbeleg mittels VSDM Prüfnachweis

Standardblauf

1. Versicherte übergeben eGK, die die Apotheker ins Kartenterminal stecken bzw. an die NFC-Schnittstelle halten
2. Das AVS ruft die Operation ReadVSD über den Konnektor auf
3. Fachdienst VSDM bildet aus KVNR und Zeitstempel mittels betreiberspezifischen Geheimnis einen Hashwert als Prüfziffer
4. Fachmodul VSDM fügt Prüfziffer dem Prüfnachweis hinzu
5. AVS übermittelt Prüfnachweis inkl. Prüfziffer an E-Rezept-Fachdienst
6. E-Rezept-Fachdienst verifiziert die Prüfziffer mit dem auch ihm bekannten Geheimnis (Hashwertvergleich) und prüft Zeitstempel auf Plausibilität

Für den Benutzer unterscheidet sich der Ablauf nicht vom PoPP.

Sicherheit und Datenschutz

- Kein PoPP-Token als eGK-Nachweis, sondern einen kryptografisch gesicherten VSDM-Prüfnachweis
- Kryptografische Absicherung über Hashwert mit geeigneter Qualitätdurch VSDM-Dienst ⇒ fälschungssichere, verlässliche Info über gesteckte eGK
- Zeitstempel ermöglicht Eingrenzung auf bestimmten Zeitraum ⇒ keine Replay-Attacken außerhalb des Zeitraums möglich
- Abruf von E-Rezepten und Vorliegen eines Prüfnachweises werden vom E-Rezept-Fachdienst protokolliert (auch fehlgeschlagene Abrufversuche bspw. mit ungültigem Prüfnachweis werden protokolliert)
- Der Konnektor protokolliert eGK-Zugriff
- Hashwert (Geheimnis) wird von VSDM-Betreiber sicher erzeugt und verwaltet
- Hashwert wird von gematik mit öffentlichem Schlüssel der VAU des E-Rezept-Servers verschlüsselt und in dieser Form an den Betreiber (IBM) weitergegeben. Der Hashwert ist dann nur in der VAU verfügbar und auch IBM selbst nicht bekannt.
- Aufruf VSDM mittels Konnektor erfolgt über Intermediär ⇒ akzeptiertes Risiko: es ist nicht erkennbar, ob die medizinische Institution, in der die eGK steckt, auch diejenige ist, die VSDM aufruft.